REMARKS

Applicant has made minor amendments to the claims, to clarify antecedents.

Applicant has amended the specification to delete reference designations and replace the reference designations with "(not shown)" since the attacking computer and the ISP are not shown nor are they needed to be shown in FIG. 1.

The examiner rejected claims 1-12, 15-32 under 35 U.S.C. 103(a) as obvious over Cox et al., U.S. Patent 6,738,814 in view of Vaidya U.S. Patent 6,279,113.

Applicant's claims are allowable over the combination of references.

Claim 1 is allowable since the references neither describe nor suggest *** sending queries to data collectors, deployed at different points in a network that carries network traffic to the data center, that sample network packets and collect statistical information on network packets sent over the network, to request the statistical information from at least some of the data collectors, the statistical information to determine the source of suspicious network traffic being sent to the data center.

The examiner contends that:

> **As to claim 1, Cox teaches a method of protecting a victim site against a denial of service attack, the method comprises: receiving from the victim site a notification that the victim site is under an attack (col. 3,. Lines 23-29, the routing device is located on the site of the victim therefore it notifies the system administrator that an attack has taken place); and Cox does not explicitly teach sending queries to data collectors, deployed at different points in a network that carries network traffic to the victim site, that sample network packets and collect statistical information on network packets sent over the network, to request the statistical information from at least some of the data collectors, the statistical information to determine the source of suspicious network traffic heir sent to the victim data center.**
>
> **Vaidya teaches detecting intrusion attempts into system resources by monitoring for attack signature. Vaidya teaches that multiple data collectors each of which includes a data monitoring device, man attack signature profile memory, and a processor are deployed at multiple sites in different segments of the network. Statistical analysis associated with an attack signature are kept in a signature profile memory and accessed by the data collectors in order to determine if the packet is associated with a network intrusion (col. 3, lines 49-65, col. 6, line 57 - col. 7, line 10).**
>
> **It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the teaching of Vaidya into the invention of Cox**

in order to maintain a statistical information on network packets in order to easily and efficiently determine network intrusion and be able to better to diagnose it.

The examiner had contended that Cox describes: "receiving from the victim site a notification that the victim site is under an attack," at Col. 3, lines 23-29. Applicant disagrees. However, Applicant has removed this limitation since it is not necessary to distinguish over the cited art.

The examiner now acknowledges that: "Cox does not explicitly teach sending queries to data collectors, deployed at different points in a network that carries network traffic to the victim site, that sample network packets and collect statistical information on network packets sent over the network, to request the statistical information from at least some of the data collectors, the statistical information to determine the source of suspicious network traffic heir sent to the victim data center."

To cure this deficiency in Cox, the examiner turned to Vaidya. Vaidya describes a network-based signature inspection network Intrusion Detection System. According to Vaidya, the data repository polls data collectors to obtain security data and to distribute attack signature profiles. [Vaidya Col. 5, lines 26-38]. Vaidya does not describe sending queries to data collectors *** to request the statistical information from at least some of the data collectors *** to determine the source of suspicious network traffic being sent to the victim data center.

Moreover, intrusion detection systems as disclosed in these references operate by using attack signatures. In contrast, claim 1 collects statistical information from plural data collectors to identify source(s) of an attack. Neither Vaidya nor Cox suggests collecting such statistical information nor do the references determine sources of an attack.

According to Vaidya, (Col. 3 lines 14-29):

Attacker 16 can also try to deny access to all external users by conducting a denial of service attack. This involves attacker 16 flooding private network 12 or routing device 10 by sending an extremely large number of packets. For example, attacker 16 may send 30,000 or more packets. According to the present invention, the attack blocking component of routing device 10 can notice that the first packet is spoofed or that it cannot be acknowledged and ignore all other packets. Further, routing device 10 can use diagnostic detection tools (e.g., trace root, ping, NS lookup) to pinpoint attacker 16 and notify the system administrator. In general, according to the present invention, routing device 10 can be enabled to intelligently

analyze incoming packets, match the packets against known patterns for attack strategies and respond accordingly to malicious packets.

Vaidya, by using attack signatures, typical of Intrusion Detection Systems identifies packets that have spoofed addresses and discards those packets. However, to "pinpoint an attacker" Vaidya relies on: "diagnostic detection tools (e.g., traceroot, ping, NS lookup)." A traceroot traces the path in the network from the originating web server over "hops" e.g., other systems to arrive at the destination. A Ping is used to send a return message to see if the destination responds and a DS likely means DNS domain name service is used to see what computer matches to the source address.

None of these techniques use statistical information from at least some of the data collectors *** to determine the source of suspicious network traffic being sent to the data center. Moreover, "traceroute," "ping," etc., as taught by Vaidya, realistically cannot be used to identify the source of spoofed traffic. Currently, there can be upwards of 4 billion possible IP addresses. In a spoofed attack, the attacker sends packets with random addresses. Traceroute, ping, etc. as taught by Vaidya cannot be used to determine the attacker's actual address. Rather, as in claim 1, by collecting statistical information from at least some of the data collectors *** to determine the source of suspicious network traffic being sent to the victim data center, traffic flows further upstream in the network are examined.

In order to support a prima facie case of obviousness, the references themselves must supply a motivation to combine their teaching, or absent such a motivation, the examiner must provide a convincing line of reasoning as to why it would be suggested to combine their teachings. The examiner contends that: "It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the teaching of Vaidya into the invention of Cox in order to maintain a statistical information on network packets in order to easily and efficiently determine network intrusion and be able to better to diagnose it."

Applicant contends that this motivation is improper to suggest the combination of these references. How can one of ordinary skill in the art be motivated to combine Cox with Vaidya "to maintain a statistical information on network packets in order to easily and efficiently determine network intrusion and be able to better to diagnose it.", when neither reference

suggests collecting the very type of data "statistical information" and use that statistical information to determine sources of an attack?

Accordingly, the combination of Vaidya and Cox is not suggested and assuming that the combination is suggested, the combination of Cox and Vaidya still neither describes nor suggests Applicant's claim 1.

Claim 15 is also allowable over Cox. Claim 15 includes the features of receiving, from a gateway disposed near the victim site, a notification that the victim data center is under an attack ... sending queries to data collectors, deployed at different points in a network that carries network traffic ... .

Claim 15 also adds the feature of determining the data center or centers involved in the attack on the victim by analyzing collected statistical information from the data collectors. The examiner does not explicitly address this feature in rejecting claim 15 over Cox and Vaidya. Rather, the examiner chooses to repeat the remarks made for claim 1, which does not include all of the features of claim 15.

Cox neither describes nor suggests receiving a notification from a gateway disposed near a victim, nor sending queries to data collectors, deployed at different points in a network, as generally argued above in claim 1. Neither Cox nor Vaidya suggests determining the data center or centers involved in the attack on the victim by analyzing collected statistical information from the data collectors.

Cox examines packets that reach a particular router that eventually routes the packets to the intended destination. Unlike the network intrusion systems disclosed in Vaidya and Cox, claim 15 requires the use of statistics collected from the data collectors that are used to determine the source of an attack and analysis of the statistical information to determine the data center(s) involved in the attack. Neither Vaidya nor Cox suggests these features.

Therefore, neither Cox nor Vaidya disclose or suggest sending queries to data collectors *** that sample network packets *** and determining the data center or centers involved in the attack on the victim by analyzing collected statistical information from the data collectors.

Claim 20 further distinguishes over Cox and Vaidya. In addition to the features of the plurality of monitors dispersed throughout a network that collect statistical data on network traffic, claim 20 also requires a control center coupled to the plurality of data collectors with the control center executing a computer program product ... to receive from the victim site a notification that the victim data center is under an attack and send queries to data collectors to request information from data collectors, the information used to determine the source of suspicious network traffic being sent to the victim. Claim 20 also adds the feature of a gateway device that passes network packets between the network and the victim site, the gateway ... coupled to the control center. Cox and Vaidya neither describe nor suggest at least these features of claim 20.

The examiner does not explicitly address all of features in rejecting claim 20 over Cox and Vaidya. Rather, the examiner chooses to repeat the remarks made for claim 1, which does not include all of the features of claim 20.

The examiner rejected claims 13 and 14 under 35 U.S.C. 103(a) as being unpatentable over Cox et al., '814 and in view of Hill et al., U.S. Patent 6,088,804.

Claims 13 and 14 are allowable at least because the base claims are allowable over the references and that Hill does not cure the deficiencies in Cox as noted in the above argument.

Further, the examiner uses Hill to teach "classifying attacks based on the severity of the attack on the network (Fig. 3, col. 2 lines 53-60; col. 6 lines 9-22)" Applicant notes that the teachings in Hill are directed to attack simulation, not to an actual attack. Nonetheless, Hill does not cure the deficiencies in Cox and these claims are also allowable.

Applicant has enclosed an Information Disclosure Statement. Applicant contends that the claims are allowable over the art in the IDS and the art of record.

Accordingly, the application is in condition for allowance and such action is respectfully requested.

Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 9/14/01

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

21131679.doc